1523

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	Criminal No. 15-233
v.	)	
	)	18 U.S.C. §§ 1037(a)(1),
	)	(b)(2)(A), and 2
RYAN NEIL GREEN,	)	
a/k/a "uid0"	)	

INFORMATION

INTRODUCTION

At all times relevant to this Information:

1. DARKODE was an Internet forum where individuals convened online to buy, sell, trade, and discuss intrusions on others' computers and electronic devices. One could only become a member of DARKODE by declaring to existing members what type of relevant ability or product he or she could bring to the forum and then being approved for membership by the other members.

2. Defendant RYAN NEIL GREEN resided in the state of Kentucky and used the Internet nickname "uid0." GREEN was a member of the Internet forum known as DARKODE.

3. Spreaders are computer code that were featured on the DARKODE forum and were created to infect large numbers of computers through the use of the social media platforms such as AOL Instant Messenger, MSN Messenger, and Facebook. Once a spreader infected a victim's computer, the malware would access the victim's AOL, MSN, or Facebook account, then the victim's contact list within that

account, and then send out spearphishing messages to each of the victim's contacts, purporting to be from the victim. If the recipient of the message clicked the weblink included within the message, a computer file would be downloaded onto the recipient's computer. When the recipient opened the computer file, the recipient's computer was then infected with malware known as "Slenfbot" and/or "Dolbot."

4. "Slenfbot" and/or "Dolbot" was "loader" malware which, when downloaded and installed onto a victim computer, would "call back" over the Internet to "command and control" computer servers controlled by the defendant and his coconspirators to download the spreader onto the recipient computer and the process would continue to the new victim's contacts list.

5. The "command and control" servers used by the conspirators belonged to unknowing third parties, and were hacked by the conspirators. Furthermore, a computer program crafted by RYAN NEIL GREEN would be placed onto the hacked "command and control" servers which enabled to them to communicate covertly with, and control, the infected computers as a botnet.

6. The defendant, RYAN NEIL GREEN, and others would sell access to the botnet to an unidentified coconspirator who would utilize the infected computers within the botnet to send high volumes of spam messages.

7. The defendant, RYAN NEIL GREEN, and others would be paid approximately $200-300 for every 10,000 active infections by the unidentified coconspirator for maintaining the size of the botnet through the constant use of the spreader.

COUNT ONE

The United States Attorney charges:

From in and around 2006, until on or about October 6, 2012, in the Western District of Pennsylvania and elsewhere, the defendant, RYAN NEIL GREEN, a/k/a "uid0," knowingly did aid, abet, and assist others, in and affecting interstate and foreign commerce, and did knowingly access a protected computer without authorization, namely a computer that had been infected through the use of a spreader by Slenfbot, and did intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer.

In violation of Title 18, United States Code, Sections 1037(a)(1), 1037(b)(2)(A) and 2.

DAVID J. HICKTON
United States Attorney
PA ID No. 34524